We claim:

Sub A5

1. In a computing environment having a connection to a network, a computer program product embodied on a computer readable medium readable by a computer in said environment, for establishing a secure, low-overhead connection between a client application and a server application using existing message types, said computer program product comprising:

computer-readable program code means for piggy-backing a request for a message encoding scheme proposal onto a first message sent from said client application to said server application, wherein said first message uses a first existing message type;

computer-readable program code means for piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second existing message type and wherein said first portion comprises a response to said request for a message encoding scheme;

computer-readable program code means for piggy-backing a second portion of security information onto a third message sent from said client application to said server application, wherein said third message uses said first existing message type; and

computer-readable program code means for piggy-backing a third portion of security information onto a fourth message sent from said server application to said client application, wherein said fourth message uses a third existing message type.

2. The computer program product according to Claim 1, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) GET message, said second existing message type is an HTTP REDIRECT message, and said third existing message type is a response to said

HTTP GET message.

3. The computer program product according to Claim 1, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) POST message, said second existing message type is an HTTP REDIRECT message, and said third existing message type is a response to said HTTP POST message.

4. The computer program product according to Claim 1, wherein said first existing message type is a Wireless Session Protocol (WSP) GET message, said second existing message type is a WSP REDIRECT message, and said third existing message type is a response to said WSP GET message.

5. The computer program product according to Claim 1, wherein said first existing message type is a Wireless Session Protocol (WSP) POST message, said second existing message type is a WSP REDIRECT message, and said third existing message type is a response to said WSP POST message.

6. The computer program product according to Claim 1, wherein:

said first message requests a secure page from said server application, wherein said secure page request further comprises an identifier of said secure page;

said second message sends a redirection message from said server application to said client application, wherein said redirection message comprises a redirected identifier of said secure

page;

said third message sends a subsequent request for said secure page from said server application in response to said redirection message, wherein said subsequent request further comprises said redirected identifier of said secure page; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

7. The computer program product according to Claim 6, wherein:

said first portion further comprises a security certificate of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

8. The computer program product according to Claim 6, wherein:

said first portion further comprises an identification of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

9. The computer program product according to Claim 7 or Claim 8, wherein said request for a message encoding scheme further comprises a keyword indicating said request.

10. The computer program product according to Claim 9, wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

11. The computer program product according to Claim 6, wherein said redirected identifier of said secure page may be identical to said identifier of said secure page.

12. The computer program product according to Claim 1, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends an authentication message from said server application to said client application;

said third message sends a subsequent request for said secure page from said server application in response to said authentication message; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

13. The computer program product according to Claim 12, wherein said authentication

message comprises a redirected identifier of said secure page, and wherein said subsequent request further comprises said redirected identifier of said secure page.

14. A system for establishing a secure, low-overhead connection between a client application and a server application using existing message types in a computing environment having a connection to a network, said system comprising:

means for piggy-backing a request for a message encoding scheme proposal onto a first message sent from said client application to said server application, wherein said first message uses a first existing message type;

means for piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second existing message type and wherein said first portion comprises a response to said request for a message encoding scheme;

means for piggy-backing a second portion of security information onto a third message sent from said client application to said server application, wherein said third message uses said first existing message type; and

means for piggy-backing a third portion of security information onto a fourth message sent from said server application to said client application, wherein said fourth message uses a third existing message type.

15. The system according to Claim 14, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) GET message, said second existing message type is an HTTP www-

Authenticate message, and said third existing message type is a response to said HTTP GET message.

16. The system according to Claim 14, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) POST message, said second existing message type is an HTTP www-Authenticate message, and said third existing message type is a response to said HTTP POST message.

17. The system according to Claim 14, wherein said first existing message type is a Wireless Session Protocol (WSP) GET message, said second existing message type is a WSP www-Authenticate message, and said third existing message type is a response to said WSP GET message.

18. The system according to Claim 14, wherein said first existing message type is a Wireless Session Protocol (WSP) POST message, said second existing message type is a WSP www-Authenticate message, and said third existing message type is a response to said WSP POST message.

19. The system according to Claim 14, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends an authentication message from said server application to said

client application;

said third message sends a subsequent request for said secure page from said server application in response to said authentication message; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

20. The system according to Claim 19, wherein said authentication message comprises a redirected identifier of said secure page, and wherein said subsequent request further comprises said redirected identifier of said secure page.

21. The system according to Claim 19 or Claim 20, wherein:

said first portion further comprises a security certificate of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

22. The system according to Claim 19 or Claim 20, wherein:

said first portion further comprises an identification of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

23. The system according to Claim 20, wherein said request for a message encoding scheme further comprises a keyword indicating said request.

24. The system according to Claim 23, wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

25. The system according to Claim 22, wherein said request for a message encoding scheme further comprises a keyword indicating said request and wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

26. The system according to Claim 20, wherein said redirected identifier of said secure page may be identical to said identifier of said secure page.

27. The system according to Claim 14, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends a redirection message from said server application to said client

application, wherein said redirection message comprises a redirected identifier of said secure page;

said third message sends a subsequent request for said secure page from said server application in response to said redirection message, wherein said subsequent request further comprises said redirected identifier of said secure page; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

28. A method for establishing a secure, low-overhead connection between a client application and a server application using existing message types in a computing environment having a connection to a network, said method comprising the steps of:

piggy-backing a request for a message encoding scheme proposal onto a first message sent from said client application to said server application, wherein said first message uses a first existing message type;

piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second existing message type and wherein said first portion comprises a response to said request for a message encoding scheme;

piggy-backing a second portion of security information onto a third message sent from said client application to said server application, wherein said third message uses said first existing message type; and

piggy-backing a third portion of security information onto a fourth message sent from said server application to said client application, wherein said fourth message uses a third existing message type.

29. The method according to Claim 28, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) GET message, said second existing message type is an HTTP www-Authenticate message, and said third existing message type is a response to said HTTP GET message.

30. The method according to Claim 28, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) POST message, said second existing message type is an HTTP www-Authenticate message, and said third existing message type is a response to said HTTP POST message.

31. The method according to Claim 28, wherein said first existing message type is a Wireless Session Protocol (WSP) GET message, said second existing message type is a WSP www-Authenticate message, and said third existing message type is a response to said WSP GET message.

32. The method according to Claim 28, wherein said first existing message type is a Wireless Session Protocol (WSP) POST message, said second existing message type is a WSP www-Authenticate message, and said third existing message type is a response to said WSP POST

message.

33. The method according to Claim 28, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends an authentication message from said server application to said client application;

said third message sends a subsequent request for said secure page from said server application in response to said authentication message; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

34. The method according to Claim 33, wherein said authentication message comprises a redirected identifier of said secure page, and wherein said subsequent request further comprises said redirected identifier of said secure page.

35. The method according to Claim 33 or Claim 34, wherein:

said first portion further comprises a security certificate of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a

public key of said client application.

36. The method according to Claim 33 or Claim 34, wherein:

said first portion further comprises an identification of said server application;

said second portion further comprises a set of information encrypted using a public key of said server application; and

said third portion further comprises a nonce of said server application, encrypted using a public key of said client application.

37. The method according to Claim 34, wherein said request for a message encoding scheme further comprises a keyword indicating said request.

38. The method according to Claim 37, wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

39. The method according to Claim 36, wherein said request for a message encoding scheme further comprises a keyword indicating said request and wherein said set of information comprises: zero or more parameters required for said secure page request; an identification of said client application; a client nonce; and optionally including a timestamp.

40. The method according to Claim 34, wherein said redirected identifier of said secure page

may be identical to said identifier of said secure page.

41. The method according to Claim 28, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page;

said second message sends a redirection message from said server application to said client application, wherein said redirection message comprises a redirected identifier of said secure page;

said third message sends a subsequent request for said secure page from said server application in response to said redirection message, wherein said subsequent request further comprises said redirected identifier of said secure page; and

said fourth message sends a response to said subsequent secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

42. A method for establishing a secure, low-overhead connection between a client application and a server application using existing message types in a computing environment having a connection to a network, said method comprising the steps of:

piggy-backing a request for said server application to select a message encoding scheme onto a first message sent from said client application to said server application, wherein said first message uses a first existing message type; and

piggy-backing a first portion of security information onto a second message sent from said

server application to said client application, wherein said second message uses a second existing message type.

43. The method according to Claim 42, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) GET message and said second existing message type is a response to said HTTP GET message.

44. The method according to Claim 42, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) POST message and said second existing message type is a response to said HTTP POST message.

45. The method according to Claim 42, wherein said first existing message type is a Wireless Session Protocol (WSP) GET message and said second existing message type is a response to said WSP GET message.

46. The method according to Claim 42, wherein said first existing message type is a Wireless Session Protocol (WSP) POST message and said second existing message type is a response to said WSP POST message.

47. The method according to Claim 42, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page; and

said second message sends a response to said secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

48. The method according to Claim 47, wherein:

said request to select a message encoding scheme further comprises an identifier of said client application, a nonce of said client application, and optionally including a timestamp; and

said first portion further comprises a set of information encrypted using a public key of said server application.

49. The method according to Claim 48, wherein said set of information further comprises:

a nonce of said server application, encrypted using a public key of said client application; and

a security certificate of said server application.

50. The method according to Claim 48 or Claim 49, wherein first message further comprises zero or more parameters required for said secure page request.

51. A system for establishing a secure, low-overhead connection between a client application and a server application using existing message types in a computing environment having a connection to a network, said system comprising:

means for piggy-backing a request for said server application to select a message encoding

scheme onto a first message sent from said client application to said server application, wherein said first message uses a first existing message type; and

means for piggy-backing a first portion of security information onto a second message sent from said server application to said client application, wherein said second message uses a second existing message type.

52. The system according to Claim 51, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) GET message and said second existing message type is a response to said HTTP GET message.

53. The system according to Claim 51, wherein said first existing message type is a Wireless Session Protocol (WSP) GET message and said second existing message type is a response to said WSP GET message.

54. The system according to Claim 51, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page; and

said second message sends a response to said secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

55. The system according to Claim 54, wherein:

said request to select a message encoding scheme further comprises an identifier of said client application, a nonce of said client application, and optionally including a timestamp; and

said first portion further comprises a set of information encrypted using a public key of said server application.

56. The system according to Claim 55, wherein said set of information further comprises:

a nonce of said server application, encrypted using a public key of said client application; and

a security certificate of said server application.

57. The system according to Claim 55 or Claim 56, wherein first message further comprises zero or more parameters required for said secure page request.

58. In a computing environment having a connection to a network, a computer program product embodied on a computer readable medium readable by a computer in said environment, for establishing a secure, low-overhead connection between a client application and a server application using existing message types, said computer program product comprising:

computer-readable program code means for piggy-backing a request for said server application to select a message encoding scheme onto a first message sent from said client application to said server application, wherein said first message uses a first existing message type; and

computer-readable program code means for piggy-backing a first portion of security

information onto a second message sent from said server application to said client application, wherein said second message uses a second existing message type.

59. The computer program product according to Claim 58, wherein said first existing message type is a HyperText Transfer Protocol (HTTP) GET message and said second existing message type is a response to said HTTP GET message.

60. The computer program product according to Claim 58, wherein said first existing message type is a Wireless Session Protocol (WSP) GET message and said second existing message type is a response to said WSP GET message.

61. The computer program product according to Claim 58, wherein:

said first message requests a secure page from said server application, wherein said request further comprises an identifier of said secure page; and

said second message sends a response to said secure page request to said client application, wherein said response further comprises a content portion encrypted using a session key generated by said server application.

62. The computer program product according to Claim 61, wherein:

said request to select a message encoding scheme further comprises an identifier of said client application, a nonce of said client application, and optionally including a timestamp; and

said first portion further comprises a set of information encrypted using a public key of

[redacted]

said server application.

63. The computer program product according to Claim 62, wherein said set of information further comprises:

a nonce of said server application, encrypted using a public key of said client application; and

a security certificate of said server application.

64. The computer program product according to Claim 62 or Claim 63, wherein first message further comprises zero or more parameters required for said secure page request.

Add A67